Information that falls within any of the categories in §§ 158.7 through 158.10 and in 44 FR 4403 shall be declassified if the designated DoD reviewer determines, in light of the declassification considerations contained in § 158.11 that classification no longer is required. In the absence of such a declassification determination, the classification of the information shall continue as long as required by national security considerations.

(e) Before any declassification or downgrading action, DoD information under review should be coordinated with the Department of State on subjects cited in § 158.12, and with the Central Intelligence Agency (CIA) on subjects cited in § 158.13.

§ 158.6 Responsibilities.

(a) The *Deputy Under Secretary of Defense for Policy* shall:

(1) Exercise oversight and policy supervision over the implementation of this part.

(2) Request DoD Components to review §§ 158.7 through 158.11 of this part every 5 years.

(3) Revise §§ 158.7 through 158.11 to ensure they meet DoD needs.

(4) Authorize, when appropriate, other Federal agencies to apply this part to DoD information in their possession.

(b) The *Head of each DoD Component* shall:

(1) Recommend changes to §§158.7 through 158.13 of this part.

(2) Propose, with respect to specific programs, projects, and systems under his or her classification jurisdiction, supplements to §§ 158.7 through 158.11 of this part.

(3) Provide advice and designate experienced personnel to provide timely assistance to the Archivist of the United States in the systematic review of records under this part.

(c) The *Director, National Security Agency/Chief, Central Security Service (NSA/CSS*), shall develop, for approval by the Secretary of Defense, special procedures for systematic review and declassification of classified cryptologic information.

(d) The *Archivist of the United States* is authorized to apply this part when reviewing DoD classified information that has been accessioned into the Archives of the United States.

§ 158.7 Categories of information that require review before declassification.

The following categories of information shall be reviewed systematically for declassification by designated DoD review in accordance with this part:

(a) Nuclear propulsion information.

(b) Information concerning the establishment, operation, and support of the U.S. Atomic Energy Detection System.

(c) Information concerning the safeguarding of nuclear materials or facilities.

(d) Information that could affect the conduct of current or future U.S. foreign relations. (Also see § 158.12.)

(e) Information that could affect the current or future military usefulness of policies, programs, weapon systems, operations, or plans when such information would reveal courses of action, concepts, tactics, or techniques that are used in current operations plans.

(f) Research, development, test, and evaluation (RDT&E) of chemical and biological weapons and defensive systems; specific identification of chemical and biological agents and munitions; chemical and biological warfare plans; and U.S. vulnerability to chemical or biological warfare attack.

(g) Information about capabilities, installations, exercises, research, development, testing and evaluation, plans, operations, procedures, techniques, organization, training, sensitive liaison and relationships, and equipment concerning psychological operations; escape, evasion, rescue and recovery, insertion, and infiltration and exfiltration; cover and support; deception; unconventional warfare and special operations; and the personnel assigned to or engaged in these activities.

(h) Information that reveals sources or methods of intelligence or counterintelligence, counterintelligence activities, special activities, identities of clandestine human agents, methods of special operations, analytical techniques for the interpretation of intelligence data, and foreign intelligence reporting. This includes information

that reveals the overall scope, processing rates, timeliness, and accuracy of intelligence systems and networks, including the means of interconnecting such systems and networks and their vulnerabilities.

(i) Information that relates to intelligence activities conducted jointly by the Department of Defense with other Federal agencies or to intelligence activities conducted by other Federal agencies in which the Department of Defense has provided support. (Also see §158.13.)

(j) Airborne radar and infrared imagery.

(k) Information that reveals space system:

(1) Design features, capabilities, and limitations (such as antijam characteristics, physical survivability features, command and control design details, design vulnerabilities, or vital parameters).

(2) Concepts of operation, orbital characteristics, orbital support methods, network configurations, deployments, ground support facility locations, and force structure.

(l) Information that reveals operational communications equipment and systems:

(1) Electronic counter-counter-measures (ECCM) design features or performance capabilities.

(2) Vulnerability and susceptibility to any or all types of electronic warfare.

(m) Information concerning electronic intelligence, telemetry intelligence, and electronic warfare (electronic warfare support measures, electronic countermeasures (ECM), and ECCM) or related activities, including:

(1) Information concerning or revealing nomenclatures, functions, technical characteristics, or descriptions of foreign communications and electronic equipment, its employment or deployment, and its association with weapon systems or military operations.

(2) Information concerning or revealing the processes, techniques, operations, or scope of activities involved in acquiring, analyzing, and evaluating the above information, and the degree of success obtained.

(n) Information concerning Department of the Army systems listed in §158.8.

(o) Information concerning Department of the Navy systems listed in §158.9.

(p) Information concerning Department of the Air Force systems listed in §158.10.

(q) Cryptologic information (including cryptologic sources and methods). This includes information concerning or revealing the processes, techniques, operations, and scope of SIGINT comprising communications intelligence, electronics intelligence, and telemetry intelligence; and the cryptosecurity and emission security components of COMSEC, including the communications portion of cover and deception plans.

(1) Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows:

(i) Those that relate to COMSEC. In documentary form, they provide COMSEC guidance or information. Many COMSEC documents and materials are accountable under the Communications Security Material Control System. Examples are items bearing transmission security (TSEC) nomenclature and crypto keying material for use in enciphering communications and other COMSEC documentation such as National COMSEC Instructions, National COMSEC/Emanations Security (EMSEC) Information Memoranda, National COMSEC Committee Policies, COMSEC Resources Program documents, COMSEC Equipment Engineering Bulletins, COMSEC Equipment System Descriptions, and COMSEC Technical Bulletins.

(ii) Those that relate to SIGINT. These appear as reports in various formats that bear security classifications, sometimes followed by five-letter codewords (World War II's ULTRA, for example) and often carrying warning caveats such as ''This document contains codeword material'' and ''Utmost secrecy is necessary . . .'' Formats may appear as messages having addressees, ''from'' and ''to'' sections, and as summaries with SIGINT content with or without other kinds of intelligence and comment.

(iii) RDT&E reports and information that relate to either COMSEC or SIGINT.

(2) Commonly used words that may help in identification of cryptologic documents and materials are ''cipher,'' ''code,'' ''codeword,'' ''communications intelligence'' or ''COMINT,'' ''communications security'' or ''COMSEC,'' ''cryptanalysis,'' ''crypto,'' ''cryptography,'' ''cryptosystem,'' ''decipher,'' ''decode,'' ''decrypt,'' ''direction finding,'' ''electronic intelligence'' or ''ELINT,'' ''electronic security,'' ''encipher,'' ''encode,'' ''encrypt,'' ''intercept,'' ''key book,'' ''signals intelligence'' or ''SIGINT,'' ''signal security,'' and ''TEMPEST.''

§ 158.8 Categories of information that require review before declassification: Department of the Army systems.

The following categories of Army information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this part.

(a) Ballistic Missile Defense (BMD) missile information, including the principle of operation of warheads (fuzing, arming, and destruct operations); quality or reliability requirements; threat data; vulnerability; ECM and ECCM); details of design, assembly, and construction; and principle of operations.

(b) BMD systems data, including the concept definition (tentative roles, threat definition, and analysis and effectiveness); detailed quantitative technical system description-revealing capabilities or unique weaknesses that are exploitable; overall assessment of specific threat-revealing vulnerability or capability; discrimination technology; and details of operational concepts.

(c) BMD optics information that may provide signature characteristics of U.S. and United Kingdom ballistic weapons.

(d) Shaped-charge technology.

(e) Fleshettes.

(f) M380 Beehive round.

(g) Electromagnetic propulsion technology.

(h) Space weapons concepts.

(i) Radar-fuzing programs.

(j) Guided projectiles technology.

(k) ECM and ECCM to weapons systems.

(l) Armor materials concepts, designs, or research.

(m) 2.75-inch Rocket System.

(n) Air Defense Command and Coordination System (AN/TSQ–51).

(o) Airborne Target Acquisition and Fire Control System.

(p) Chaparral Missile System.

(q) Dragon Guided Missile System Surface Attack, M47.

(r) Forward Area Alerting Radar (FAAR) System.

(s) Ground laser designators.

(t) Hawk Guided Missile System.

(u) Heliborne, Laser, Air Defense Suppression and Fire and Forget Guided Missile System (HELLFIRE).

(v) Honest John Missile System.

(w) Lance Field Artillery Missile System.

(x) Land Combat Support System (LCSS).

(y) M22 (SS–11 ATGM) Guided Missile System, Helicopter Armament Subsystem.

(z) Guided Missile System, Air Defense (NIKE HERCULES with Improved Capabilities with HIPAR and ANTIJAM Improvement).

(aa) Patriot Air Defense Missile System.

(bb) Pershing IA Guided Missile System.

(cc) Pershing II Guided Missile System.

(dd) Guided Missile System, Intercept Aerial M41 (REDEYE) and Associated Equipment.

(ee) U.S. Roland Missile System.

(ff) Sergeant Missile System (less warhead) (as pertains to electronics and penetration aids only).

(gg) Shillelagh Missile System.

(hh) Stinger/Stinger-Post Guided Missile System (FIM–92A).

(ii) Terminally Guided Warhead (TWG) for Multiple Launch Rocket System (MLRS).

(jj) TOW Heavy Antitank Weapon System.

(kk) Viper Light Antitank/Assault Weapon System.